UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/761,920	01/20/2004	Vincent Piel	500110459-2	4097

22879 7590 07/10/2008

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
PATEL, NIRAV B	
ART UNIT	PAPER NUMBER
2135	

NOTIFICATION DATE	DELIVERY MODE
07/10/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/761,920
Filing Date: January 20, 2004
Appellant(s): PIEL, VINCENT

Charles W. Griggers
Reg. No. 47,283
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed April 28, 2008 appealing from the Office action mailed Sep. 27, 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Herzi (US Patent No. 6,484,262 – Jan. 26, 1999)

Hamamoto et al. (US Pub. No. 2002/0000913 A1 – May 16, 2001)

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herzi (US 6,484,262) and in view of Hamanoto et al (US Pub. No. 2002/0000913).

As per claims 1, 10, 11, 12 and 17, Herzi teaches a component, a BIOS and a firmware element for a computer, the component, BIOS comprising a firmware element operable to perform a security check to verify the computer is connected to an authorised network, the security check comprising the steps of (Abstract, Figs 1-3 and associated texts):

generating a random number, encrypting the random number with a public key of a public/private key pair associated with the network, transmitting the encrypted random number to a network device via the network (col. 4, lines 58-64, col. 5, lines 15-25), receiving a response comprising a number from the network device (col. 4, line 65 through col. 5, line 7), and permitting operation of at least a subsystem of the computer if the response is in accordance with the random number, the step of permitting operation of at least a subsystem of the computer if the response is in accordance with the

random number comprises comparing the random number transmitted to the network device with the number in the response and permitting operation if the number in the response matches the random number transmitted to the network device (col. 5, lines 8-15).

Herzi teaches that the security check is performed is implemented upon every boot of the particular computer system or at regular intervals of times etc. as established for a given security policy. Herzi doesn't expressively mention that the security check is performed when the computer is detected to have been in an unpowered state.

Hamamoto teaches the security check is performed when the computer is detected to have been in an unpowered state since a previous security check [paragraph 0006].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Hamamoto with Herzi to perform the security check even if the computer is detected in an unpowered state, since one would have been motivated to improve the reliability for the security of the computer/machine even if the computer/machine itself has been stolen (or unpowered) [paragraph 0005].

As per claims 2 and 13, Herzi teaches a component and a computer according to claims 1 and 12 respectively, wherein the firmware element comprises a BIOS (col. 3, lines 18-34)

As per claims 3 and 14, Herzi teaches a component and a computer according to claims 2 and 13 respectively, wherein the firmware element is operable to perform a security check as part of a boot process (col. 2, lines 56-64, col. 3, lines 64-67).

As per claims 4 and 15, Herzi teaches a component and a computer according to claims 2 and 13 respectively, wherein the firmware element is operable to prevent operation of the computer if a valid response is not received (col. 5, lines 37-46).

As per claims 5 and 16, Herzi teaches a component and a computer according to claims 2 and 13 respectively wherein the BIOS comprises a boot block and wherein the firmware element is stored in the boot block (col. 2, lines 56-64).

As per claim 6, Herzi teaches a component according to claim 1 wherein the firmware element comprises a controller for a peripheral (col. 3, lines 53-63, i.e. without authorization, the BIOS of the computer system halts all practical operation of the computer system).

As per claim 7, Herzi teaches a component according to claim 6 wherein the firmware element is operable to perform a security check in response to a transition to an operating state (col. Col. 2, lines 58-61, i.e. security measure is implemented by the processor prior to booting up of the operating system).

As per claim 8, Herzi teaches a component according to claim 6 wherein the firmware element is operable to prevent operation of the peripheral if a valid response is not received (col. 3, lines 53-63, i.e. without authorization, the BIOS of the computer system halts all practical operation of the computer system).

As per claim 9, Herzi teaches a component according to claim 6 wherein a network enquiry to verify the computer is connected to the authorised network is transmitted to BIOS of the computer for

transmission to the network device (col. 3, lines 19-21, where the security measure of the BIOS enables the processor 20 to communicate an authentication request to the prescribed network server 14).

(10) Response to Argument

A. Regarding to Appellant's Arguments to Claims 1-9: Hamamoto does not describe that a security check is performed **when a computer is detected to have been in an unpowered state** since a previous security check, as a result, Hamamoto individually or in combination with Herzi does not teach or suggest "*permitting operation of at least….the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check*" **[*Appeal Brief* - *page 10, 11*]**. To support this limitation, Appellant pointed out the specification page 3, lines 27-29 and page 4 lines 25-30 **[**Appeal Brief, page 8 – ***Applicant's Specification:*** "……the ***security check will be performed only when the computer may have been unplugged, indicating that the computer 10 has been potentially removed from its original location***."**]**.

Examiner maintains since, Herzi's invention relates to **security of a computer system**, which provides an improved security measure against undesired theft of computer system. A computer system having network controlled security administered, where the security measure is implemented by the processor **prior to a booting up of the operating system**. Further, Herzi

teaches, as shown in Fig. 3, the BIOS creates a special packet containing a Network Authentication Request message, which includes at least an identity (e.g. serial number, asset tag number or the like) and transmits to the host system **[col. 4 lines 58-64, col. 5 lines 1-6, Fig. 3].** The host system validates the message and sends the authentication response to the BIOS firmware. If the network controlled security authentication response is a valid response, then BIOS allows a power on self test and operating system booting (i.e. a normal operation of the computer system continue – permitting operation of at least a subsystem of the computer if the response is valid) **[col. 5 lines 8-67, i.e.** Booting up of the operating system by the processor is controlled in response to the security measure, **col. 1 lines 45-49, col. 2 lines 56-64].** Therefore, Herzi teaches the claim limitation "permitting operation of .....if the response is in accordance with.....", wherein **the security measure mechanism** for the BIOS firmware in the computer system, wherein the security measure is implemented prior to a booting up of the operating system and/or at security check interval **[col. 2 lines 56-64, col. 4 lines 15-20]**. Further, in an analogous art, Hamamoto discloses a **monitoring device for security** in automatic teller machine (computer system) which comprises a plurality of processing units **[Fig. 1]**. Hamamoto's invention provide a monitoring device for security in an computer system which is capable **to monitor for security, even the computer system is in a power-off state or even if the system is powered down (i.e. when a power cord plug is removed) [paragraph 0004, 0006]**. Regarding to appellant's remark (page 11) that a backup power supply is used whenever the main power supply is unavailable, Examiner would like to clarify that the backup power supply is **only for providing power to the security monitoring units** when the **main power supply of the computer system is detected unplugged or removed [paragraph 0024, Fig. 1]**, thus, the computer system itself is as a no power state, which meets the claimed limitation.

Therefore, Hamamoto teaches the **security measure mechanism** for the computer system, even if the computer system is in an unpowered state. In this case, the combination of Herzi and Hamamoto teaches the claim limitation ".....wherein the security check is performed when the computer is detected to have been in unpowered state...." It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the system of Herzi with the teaching of Hamamoto to monitor the computer system even if the computer system is in unpowered state. Furthermore, the examiner recognizes that obviousness can also be established by combining or modifying the teaching of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to on of ordinary skill in the art. See *In re Fine*, 837 F. 2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and In re Jones, 958 F.2d 347, 21 USPQ 2nd 1941 (Fed. Cir 1992). In this case, the combination is of Herzi and Hamamoto is sufficient as one of ordinary skill in the art at the time the invention was made, since one would have been motivated to improve the reliability for the security of the computer system even if the computer system is in unpowered state or is removed from the its original location **[Hamamoto, paragraph 0005]**.

B. Regarding to Appellant's Arguments to Claim 10: Hamamoto does not describe that, "..... a security check is performed **when a computer is detected to have been in an unpowered state** since a previous security check, as a result, Hamamoto individually or in combination with Herzi does not teach or suggest "....*the security check is performed when the computer is detected to have been in an unpowered state since a previous security check*" **[*Appeal Brief - page 13, 14*]**.

Please refer to section "A" above.

C. Regarding to Appellant's Arguments to Claim 11: Hamamoto does not describe that, "….. a security check is performed **when a computer is detected to have been in an unpowered state** since a previous security check, as a result, Hamamoto individually or in combination with Herzi does not teach or suggest "*preventing continuation of the boot process….the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check* **" [Appeal Brief -** *page 15, 16*].

Please refer to section "A" above.

D. Regarding to Appellant's Arguments to Claims 12-16: Hamamoto does not describe that, "….. a security check is performed **when a computer is detected to have been in an unpowered state** since a previous security check, as a result, Hamamoto individually or in combination with Herzi does not teach or suggest "*permit operation of at least….the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check*" **[Appeal Brief -** *page 18, 19*].

Please refer to section "A" above.

E. Regarding to Appellant's Arguments to Claim 17: Hamamoto does not describe that, "….. a security check is performed **when a computer is detected to have been in an unpowered state** since a previous security check, as a result, Hamamoto individually or in combination with Herzi does not teach or suggest "*permitting operation of at least….the security check is performed in response to the computer being detected to have been in an unpowered state since a previous security check*" **[Appeal Brief -** *page 21, 22*].

Please refer to section "A" above.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Nirav Patel/

Patel Nirav
Patent Examiner GAU 2135
July 2, 2008

Conferees:

/KimYen Vu/

Supervisory Patent Examiner, Art Unit 2135

/Song, Hosuk/
Primary Examiner 2135